WE CLAIM:

1. A computer program product carrying a computer program operable to control a computer to detect malware within a computer file, said computer program comprising:

identifying code operable to identify said computer file as potentially being a specific known malware free computer file;

determining code operable to determine one or more attributes of said computer file; and

comparing code operable to compare said one or more attributes determined from said computer file with corresponding stored attributes of said specific known malware free computer file; wherein

if said attributes match, then confirming said computer file as being said specific known malware free computer file; and

if said attributes do not match then performing further malware detection processing upon said computer file.

2. A computer program product as claimed in claim 1, wherein said identifying code is operable to compare one or more of file name, storage location and file size of said computer file with a corresponding one or more of file name, storage location and file size of said specific known malware free computer file.

3. A computer program product as claimed in claim 1, wherein said computer file is identified as being potentially one specific known malware free computer file from among a plurality of specific known malware free computer files.

4. A computer program product as claimed in claim 1, wherein said one or more attributes include one of more of:

a checksum calculated from at least a portion of said computer file; and

content of at least a portion of said computer file.

5. A computer program product as claimed in claim 1, wherein said further malware detection processing includes detecting within said computer file one or more characteristic corresponding to a known malware file.

6. A computer program product as claimed in claim 5, wherein said one or more characteristic corresponding to a known malware file are stored within a malware signature file.

7. A computer program product as claimed in claim 1, wherein said specific known malware free computer file is one of:

an operating system file;

a help file; and

a malware detection software file.

8. A computer program product as claimed in claim 1, wherein said malware being detected is one or more of:

a computer virus;

a computer worm;

a computer Trojan;

a banned computer file; and

a computer file containing banned data.

9. A method of detecting malware within a computer file, said method comprising the steps of:

identifying said computer file as potentially being a specific known malware free computer file;

determining one or more attributes of said computer file; and

comparing said one or more attributes determined from said computer file with corresponding stored attributes of said specific known malware free computer file; wherein

if said attributes match, then confirming said computer file as being said specific known malware free computer file; and

if said attributes do not match then performing further malware detection processing upon said computer file.

10. A method as claimed in claim 9, wherein said step of identifying compares one or more of file name, storage location and file size of said computer file with a corresponding one or more of file name, storage location and file size of said specific known malware free computer file.

11. A method as claimed in claim 9, wherein said computer file is identified as being potentially one specific known malware free computer file from among a plurality of specific known malware free computer files.

12. A method as claimed in claim 9, wherein said one or more attributes include one of more of:

a checksum calculated from at least a portion of said computer file; and

content of at least a portion of said computer file.

13. A method as claimed in claim 9, wherein said further malware detection processing includes detecting within said computer file one or more characteristic corresponding to a known malware file.

14. A method as claimed in claim 13, wherein said one or more characteristic corresponding to a known malware file are stored within a malware signature file.

15. A method as claimed in claim 9, wherein said specific known malware free computer file is one of:

an operating system file;

a help file; and

a malware detection software file.

16. A method as claimed in claim 9, wherein said malware being detected is one or more of:

a computer virus;

a computer worm;

a computer Trojan;

a banned computer file; and

a computer file containing banned data.

17. Apparatus for detecting malware within a computer file, said apparatus comprising:

identifying logic operable to identify said computer file as potentially being a specific known malware free computer file;

determining logic operable to determine one or more attributes of said computer file; and

comparing logic operable to compare said one or more attributes determined from said computer file with corresponding stored attributes of said specific known malware free computer file; wherein

if said attributes match, then confirming said computer file as being said specific known malware free computer file; and

if said attributes do not match then performing further malware detection processing upon said computer file.

18. Apparatus as claimed in claim 17, wherein said identifying logic is operable to compare one or more of file name, storage location and file size of said computer file with a corresponding one or more of file name, storage location and file size of said specific known malware free computer file.

19. Apparatus as claimed in claim 17, wherein said computer file is identified as being potentially one specific known malware free computer file from among a plurality of specific known malware free computer files.

20. Apparatus as claimed in claim 17, wherein said one or more attributes include one of more of:

a checksum calculated from at least a portion of said computer file; and

content of at least a portion of said computer file.

21. Apparatus as claimed in claim 17, wherein said further malware detection processing includes detecting within said computer file one or more characteristic corresponding to a known malware file.

22. Apparatus as claimed in claim 21, wherein said one or more characteristic corresponding to a known malware file are stored within a malware signature file.

23. Apparatus as claimed in claim 17, wherein said specific known malware free computer file is one of:

an operating system file;

a help file; and

a malware detection software file.

24. Apparatus as claimed in claim 17, wherein said malware being detected is one or more of:

a computer virus;

a computer worm;

a computer Trojan;

a banned computer file; and

a computer file containing banned data.